

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2001273211 A

(43) Date of publication of application: 05.10.01

(51) Int. Cl. G06F 13/00
H04L 12/22
H04L 12/24
H04L 12/56
H04L 12/58

(21) Application number: 2001037593

(22) Date of filing: 14.02.01 -

(30) Priority: 15.02.00 US 2000 504157

(71) Applicant: HEWLETT PACKARD CO <HP>

(72) Inventor: SIT ERIC N
CLOUGH JAMES
NELSON DEAN S

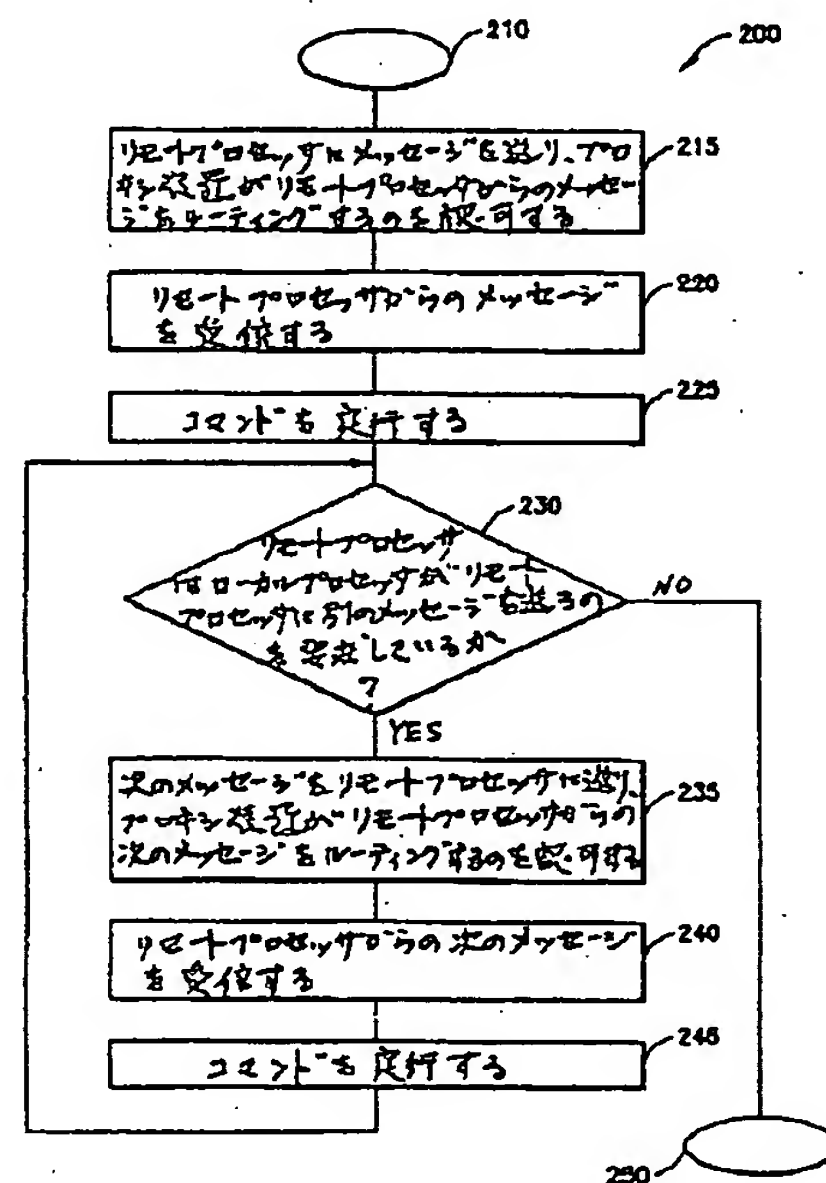
(54) METHOD AND DEVICE FOR CONTROLLING
DEVICE INSIDE FIREWALL FROM OUTSIDE

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method for enabling a remote processor to communicate with a local processor through a computer network and a firewall.

SOLUTION: The remote processor is connected to the local processor through a reverse proxy device, the computer network, the firewall and a proxy agent device. By dispatching a local request message to the proxy agent device, the local processor establishes a communication channel with the remote processor. The proxy agent device makes a response received from the local processor seem like a request and converts a response received from the firewall into a request. Similarly, the reverse proxy device converts a request received from the firewall into a response and makes a request received from the remote processor seem like a response.

COPYRIGHT: (C)2001,JPO



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2001-273211

(P2001-273211A)

(43)公開日 平成13年10月5日(2001.10.5)

(51)Int.Cl. ⁷	識別記号	F I	テーマト(参考)
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z
H 0 4 L 12/22		H 0 4 L 12/22	
12/24		12/24	
12/56		12/56	A
12/58	1 0 0	12/58	1 0 0 A

審査請求 未請求 請求項の数1 O L (全 11 頁)

(21)出願番号 特願2001-37593(P2001-37593)
(22)出願日 平成13年2月14日(2001.2.14)
(31)優先権主張番号 5 0 4 1 5 7
(32)優先日 平成12年2月15日(2000.2.15)
(33)優先権主張国 米国 (U S)

(71)出願人 398038580
ヒューレット・パカード・カンパニー
HEWLETT-PACKARD COM
PANY
アメリカ合衆国カリフォルニア州パロアル
ト ハノーバー・ストリート 3000
(72)発明者 エリック・エヌ・シット
アメリカ合衆国ニュージャージー州ウァッ
チング クレストウッド・ドライブ
115
(74)代理人 100078053
弁理士 上野 英夫

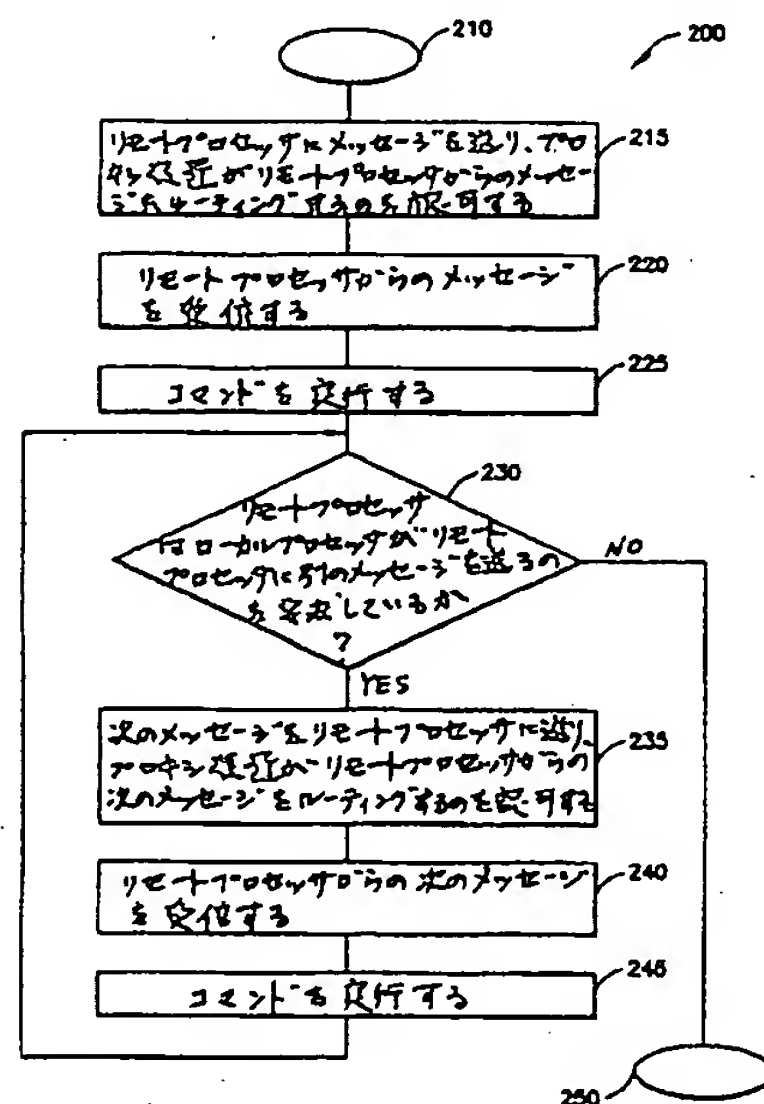
最終頁に続く

(54)【発明の名称】 ファイヤウォール内部の装置を外部から制御する方法及び装置

(57)【要約】

【課題】 リモートプロセッサが、コンピュータネットワ
ークとファイヤウォールとを介して、ローカルプロセッ
サと通信できるようにする方法を提供する。

【解決手段】 本発明の一実施例によれば、リモートプロ
セッサは、リバースプロキシ装置と、コンピュータネット
ワークと、ファイヤウォールと、プロキシエージェント
装置とを介してローカルプロセッサに結合される。ロー
カルプロセッサは、プロキシエージェント装置にロー
カル要求メッセージをディスパッチすることにより、リ
モートプロセッサとの通信チャネルを確立する。プロキ
シエージェント装置はローカルプロセッサから受信した
応答を要求のように見せるとともに、ファイヤウォール
から受信した応答を要求に変換する。同様に、リバース
プロキシ装置は、ファイヤウォールから受信した要求を
応答に変換するとともに、リモートプロセッサから受信
した要求を応答のように見せる。



【特許請求の範囲】

【請求項1】 リモートプロセッサが、リバースプロキシ装置と、コンピュータネットワークと、ファイヤウォールと、プロキシエージェント装置とを介してローカルプロセッサに結合される場合に、前記リモートプロセッサが前記ローカルプロセッサと通信できるようにするトンネリング動作を可能にするための方法であって、

ローカル要求メッセージを前記プロキシエージェント装置にディスパッチさせて前記リモートプロセッサとの通信チャネルを確立するよう、前記ローカルプロセッサを制御するステップであって、前記プロキシエージェント装置は前記ファイヤウォールと前記ネットワークとを介して前記ローカル要求メッセージを前記リバースプロキシ装置にディスパッチし、前記ファイヤウォールは前記プロキシエージェント装置によって前記ローカル要求メッセージに対するリモート応答メッセージを受信することができるようになされる、制御ステップと、

前記通信チャネルの確立に基づき、前記リモートプロセッサが前記リバースプロキシ装置にリモート要求メッセージを送出するのを可能にし、次に、前記リバースプロキシ装置が、前記リモート要求メッセージの中に含んだリモート応答メッセージをディスパッチするのを可能にするステップと、

前記ファイヤウォールを介して前記プロキシエージェント装置が前記リモート応答メッセージを受信したときに、前記リモート要求メッセージを抽出して該リモート要求メッセージを前記ローカルプロセッサにディスパッチするよう前記プロキシエージェント装置を制御するステップと、

を備えて成り、前記プロキシエージェント装置及び前記リバースプロキシ装置が、前記ローカルプロセッサまたは前記リモートプロセッサのいずれかにおける通信アプリケーションを変更することなく、前記トンネリング動作を可能にすることを特徴とする方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ファイヤウォールを通過するメッセージ転送に関し、より詳細には、ファイヤウォールによって保護される装置が、ファイヤウォールの外部にある装置によって制御できるようにする方法に関する。

【0002】

【従来の技術】 多くの場合、コンピュータデータ処理システムは、ローカル・エリア・ネットワーク（LAN）内で、プロセッサ或いはサーバに接続される、プリンタのような一群の周辺機器を備える。プロセッサ上で動作するソフトウェアによって、利用者は、動作パラメータを構成し、ローカルに接続される全ての周辺機器の動作をモニタすることが可能になる。

【0003】 一般に、コンピュータシステムによって提

供される特徴及び利便性が向上するのに応じて、システムを制御するソフトウェアは益々精巧で、複雑になる。システムのインストール及びトラブルシューティングは、システム及び周辺機器の専門知識を必要とする場合が多い。問題を突き止める場合、システムの利用者は、この専門知識を持つ技術サポートエンジニアから支援を受けなければならない。

【0004】 利用者が最初に支援を求めるのは、典型的にはサービスセンタに電話することであり、技術サポート担当者とは話をすることである。担当者は最初に、問題になっている特定のシステムの構成に関して、利用者から情報を聴取し、その後インストール及びトラブルシューティング手順を通して、利用者を誘導する。

【0005】 電話による技術サポートは、大抵の場合に時間と費用がかかる。また利用者及び技術担当者のいずれにおいてもリソースを必要とし、長距離電話による通話を伴う場合もある。成功させるためには、利用者及び担当者は、長時間の会話をし続け、技術情報及び指示を交換できなければならない。この解決は、会話による疎通がうまくいかなかったり、或いは利用者及び担当者が十分な訓練を受けていないことによって間違いが起こりやすい。最も良好な場合であっても、成功する保証はない。電話による技術サポートのやり取りが失敗すれば、利用者には、不快感から完全な失望感までの様々な感情が残り、サポートを提供する企業のイメージを損なう恐れもある。

【0006】 担当者が最初に問題のシステムにアクセスしている場合には、技術サービスは改善される。これは、そのシステムが設置されている場所へ移動することによりなし得るが、必然的にその場所への行き来に費用がかかる。好ましい別の形態では、担当者がそのシステムにリモートアクセスすることである。

【0007】 インターネットは、遠隔して位置するコンピュータが互いに情報を交換することができるチャネルを提供する。第1のコンピュータが、インターネット内で情報の要求を、第2のコンピュータに送出することができる。その後、第2のコンピュータは、所望の情報を含むメッセージで応答する。

【0008】 セキュリティ及びシステムの保全性のため、多くの組織は、その組織の外部にあるコンピュータとの情報の交換を制限するファイヤウォールを導入している。ファイヤウォールは、不要な受信要求及び情報を遮断するために、ローカルコンピュータシステムとインターネットとの間に介在する。その結果、ファイヤウォールによって保護されるローカルコンピュータシステムに、遠隔した場所から無条件にアクセスすることはできない。

【0009】 図1を参照すると、ローカルコンピュータ50とリモートコンピュータ70がインターネット65を介して接続される。プロキシ装置60は、ローカルコ

10

20

30

40

50

ンピュータ50とインターネット65との間に介在し、動作する。

【0010】プロキシ装置60は、ローカルコンピュータ50に代わってインターネット65とのインターフェースを形成し、認可を受けた場合にのみ、メッセージをインターネット65からローカルコンピュータ50にルーティングする。例として、ローカルコンピュータ50が、プロキシ装置60を介して、リモートコンピュータ70に要求75を送出することにより、リモートコンピュータ70との通信を開始する。要求75は、プロキシ装置60がリモートコンピュータ70からローカルコンピュータ50にメッセージをルーティングするのを認可する、ハイパーテキスト転送プロトコル（HTTP）ヘッダ内のプロキシ情報を含む。その後、リモートコンピュータ70が応答80を送出し、プロキシ装置60がその応答80をローカルコンピュータ50にルーティングする。

【0011】プロキシ装置60は、認可されていないメッセージがインターネット65からローカルコンピュータ50にルーティングされるのを防ぐことによって、ローカルコンピュータ50の保全性を保護するためのファイアウォールとして機能する。プロキシ装置60は認可されていない受信情報を遮断するだけでなく、遮断しなければローカルコンピュータ50が応答してしまうような、認可を受けずに受信した要求も遮断する。従って、リモートコンピュータ70は、無条件には、ローカルコンピュータ50との間でデータを読み書きすることができない。

【0012】ローカルコンピュータ50は、プロキシ装置60が受信メッセージを受け取るのをメッセージ毎に認可しなければならないため、リモートコンピュータ70からローカルコンピュータ50への各メッセージは、ローカルコンピュータ50によって開始されなければならない。いくつかのメッセージが交換される状況では、要求及び応答のパターンが必要とされる。ローカルコンピュータ50は要求75を送出し、応答76を受信し、要求77を送出し、応答78を受信し、要求79を送出し、応答80を受信する、というようなパターンが続く。一般的な場合には、ローカルコンピュータ50は、リモートコンピュータ70への要求を送出し、リモートコンピュータ70から応答を受信する。

【0013】技術サポート担当者が、遠隔して配置されているコンピュータシステムを管理したい場合がある。リモートアクセスを通して、担当者は、システムサイトの利用者の側からほとんど、或いは全く介入することなく、システムを構成し、モニタし、トラブルシューティングすることができる。さらに、担当者には、そのコンピュータシステムへの担当者のアクセスを制限するファイアウォールによって保護されているコンピュータシステムにアクセスする必要がある場合もある。

【0014】

【発明が解決しようとする課題】本発明の目的は、リモートコンピュータシステムが、インターネットを介して、ファイアウォールがインターネットとローカルコンピュータシステムとの間に介在して動作するローカルコンピュータシステムにアクセスするための方法を提供する。

【0015】本発明の別の目的は、リモートコンピュータシステムが、インターネットを介してローカルコンピュータシステムに通信するための方法を提供し、その方法では、インターネットとローカルコンピュータシステムとの間に介在して動作し、ローカルコンピュータシステム或いはリモートコンピュータシステムのいずれかにおいて動作するアプリケーションを変更する必要がある制御機能を付与することにより、そのような通信を制御する。

【0016】

【課題を解決するための手段】本発明は、リモートプロセッサが、リバースプロキシ装置と、コンピュータネットワークと、ファイアウォール装置と、プロキシエージェント装置とを介して、ローカルプロセッサに接続される場合に、リモートプロセッサがローカルプロセッサと通信できるようにするトンネリング動作を可能にする。最初に、ローカルプロセッサは、プロキシエージェント装置にローカル要求メッセージをディスパッチすることにより、リモートプロセッサとの通信チャネルを確立する。プロキシエージェント装置は、ファイアウォール及びネットワークを介してローカル要求メッセージをリバースプロキシ装置にディスパッチし、それにより、ファイアウォールが、そのローカル要求メッセージへのリモート応答メッセージを受信できるようにする。その後、リモートプロセッサはリモート要求メッセージをリバースプロキシ装置に送り、次にリバースプロキシ装置はリモート要求メッセージの中に含んだリモート応答メッセージを、ファイアウォールにディスパッチする。（ファイアウォールを介して）リモート応答メッセージがプロキシエージェント装置によって受信されると、プロキシエージェント装置は、ローカルプロセッサへのリモート要求メッセージを抽出し、ディスパッチする。ローカルプロセッサによるローカル応答メッセージのディスパッチによって、プロキシエージェントは、ローカル応答メッセージをローカル要求メッセージに組み込み、ファイアウォール及びリバースプロキシ装置を介して、リモートプロセッサにローカル要求メッセージをディスパッチできるようにする。

【0017】

【発明の実施の形態】従来からのインターネット用語において、かつハイパーテキスト転送プロトコル（HTTP）に従えば、「要求」は、第2のプロセッサからの情報を求める第1のプロセッサによって発行されるメッセ

10

20

30

40

50

ージであり、「応答」は、要求された情報を含む、第2のプロセッサから第1のプロセッサへのメッセージである。通常、ファイアウォールの後ろで保護されて、プロセッサは要求を発行し、応答を受信する。本発明では、ローカルプロセッサはリモートプロセッサへの第1の要求を行うが、その後、リモートプロセッサからのメッセージは「要求」になり、リモートプロセッサへのメッセージは「応答」になる。こうして、ファイアウォール外部の装置管理を行うためのリバース（逆）HTTP接続が確立される。

【0018】図2は、特に本発明を実行するように構成されたコンピュータシステムのブロック図である。一群の周辺機器110が、LAN112内のローカルプロセッサ122に接続される。ローカルコンピュータ120は、プロキシ装置145を介してインターネット150に接続される。リモートコンピュータ155もインターネット150に接続される。

【0019】ローカルコンピュータ120は、ローカルプロセッサ122と、コンピュータメモリ（図示せず）と、クライアント装置管理ゲートウェイ（CDMG）125とを備える。CDMG125は、ローカルプロセッサ122を制御して、本発明の方法を実行する。リモートコンピュータ155は、リモートプロセッサ157と、装置110を制御するためにCDMG125と通信を行うサポートアプリケーション160とを備える。

【0020】CDMG125は、ローカルプロセッサ122を制御して、プロキシ装置145を介してリモートプロセッサ157に要求170を送出することにより、リモートプロセッサ157との通信を開始する。要求170は典型的には、ローカルプロセッサ122と装置110とを識別する情報を含むであろう。要求170はまた、プロキシ装置145がリモートプロセッサ157からローカルプロセッサ122にメッセージをルーティングするのを認可するHTTPヘッダのプロキシ情報も含む。その後、リモートプロセッサ157は、プロキシ装置145がローカルプロセッサ122にルーティングする要求171を送出することにより応答する。要求171は、要求170への有効な応答であることに留意されたい。

【0021】要求171は、装置110に対してローカルプロセッサ122によって実行されることになる1つ或いは複数のコマンドを指示するメッセージである。例えば、コマンドは、装置110が再度初期化されるべきであることを示すことができる。また要求171は、リモートプロセッサ157に情報を送出的ように、ローカルプロセッサ122を指示することができる。例えば、サポートアプリケーション160は、ローカルプロセッサ122或いは装置110の構成に関する付加情報を必要とする場合もある。ローカルプロセッサ122は、応答172において要求された情報を送出的。

【0022】応答172は、プロキシ装置145がリモートプロセッサ157からローカルプロセッサ122に、別の「応答」メッセージをルーティングするのを認可するHTTPヘッダのプロキシ情報を含む。その後、リモートプロセッサ157は、プロキシ装置145がローカルプロセッサ122にルーティングする要求173を送出する。要求173は、装置110に対して実行されるべきコマンドを指示することができ、リモートプロセッサ157にさらに情報を与えるためにローカルプロセッサ122を指示することもできる。要求173が、ローカルプロセッサ122が付加情報を送出的よう指示する指示を含む場合には、ローカルコンピュータは応答174において付加情報を送出的。

【0023】要求170が送出的された後、要求及び応答のパターンが明らかになることに留意されたい。一般的な場合には、リモートプロセッサ157はローカルプロセッサ122に要求を送出し、ローカルプロセッサ122から応答を受信する。このパターンは、図1に示されるパターンの反対である。ローカルプロセッサ122によってリモートプロセッサ157に送出的される各メッセージ（要求170及び応答172、174）は、プロキシ装置145がリモートプロセッサ157からローカルプロセッサ122にメッセージ（要求171、173）をルーティングするのを認可するHTTPヘッダのプロキシ情報を含む。それによって装置110は、リモートプロセッサ157によって間接的に制御される。

【0024】CDMG125は、キーボードのような任意の標準的なユーザインターフェースを介して適用される通信開始コマンド130に応答して、リモートプロセッサ157との通信を開始するであろう。これは例えば、ローカルプロセッサ122の利用者が、装置110をインストール或いはトラブルシューティングする支援を必要とする場合に相当するであろう。

【0025】またCDMG125は、電子メール（Eメール）を介して受信した通信開始コマンド140に応答して通信を開始するであろう。簡易メール転送プロトコル（SMTP）を用いて、リモートプロセッサ157は、通信開始要求165AとしてEメールサーバ135に格納される通信開始要求165を送出することができる。通信開始要求165（及び165A）は、通信開始コマンド140を含む。通信開始コマンド140は、Eメールサーバ135を定期的にポーリングするCDMG125によって、通信開始要求165AがEメールサーバ135から読み出される際に実行される。通信開始要求165は、例えば、装置110の性能が、サポートアプリケーション160によって定期的に評価、かつ較正される場合に用いることができる。また第三者（図示せず）が装置110を自動的にモニタし、較正するための機会を与えることができる。

【0026】CDMG125を起動して通信を開始する

ための第3の方法は、装置110A内からの通信開始コマンド113によって生成可能である。通信開始コマンド113は、セルフテストを通して自動的に実行し、異常を検出するか、或いは定期的にメンテナンスプログラムを実行する場合に用いられる。装置110Aは、通信開始コマンド113をCDMG125に発行し、その後CDMG125は、リモートプロセッサ157との通信を開始し、装置110Aの自動テスト及び較正を開始する。

【0027】図3は、本発明を実行するためのコンピュータシステムの別の実施形態のブロック図である。装置110bは、プロキシ装置145を介してインターネット150に接続される。リモートコンピュータ155もインターネット150に接続される。

【0028】装置110bは、ローカルプロセッサ122Aと、コンピュータメモリ（図示せず）と、クライアント装置管理ゲートウェイ（CDMG）125Aとを備える。CDMG125Aは、ローカルプロセッサ122Aを制御して、本発明の方法を実行する。リモートコンピュータ155は、リモートプロセッサ157と、装置110bを制御するためにCDMG125Aと通信を行うサポートアプリケーション160とを備える。

【0029】通信開始コマンド113Aは、装置110bがセルフテストを通して自動的に実行し、異常を検出するか、或いは定期的にメンテナンスプログラムを実行する場合に生成される。通信開始コマンド113Aは、CDMG125を起動し、リモートプロセッサ157との通信を開始する。

【0030】CDMG125Aはローカルプロセッサ122Aを制御して、プロキシ装置145を介してリモートプロセッサ157に要求170を送出することにより、リモートプロセッサ157との通信を開始する。要求170は典型的には、ローカルプロセッサ122A及び装置110bを識別する情報を含むであろう。また要求170は、プロキシ装置145がリモートプロセッサ157からローカルプロセッサ122Aにメッセージをルーティングするのを認可するHTTPヘッダのプロキシ情報も含む。その結果、リモートプロセッサ157は、要求171を送出することにより応答し、その応答を、プロキシ装置145がローカルプロセッサ122Aにルーティングする。要求171は、要求170への有効な応答であることに留意されたい。

【0031】要求171は、装置110bに対して、ローカルプロセッサ122Aによって実行されるべき1つ或いは複数のコマンドを指示するメッセージである。例えば、コマンドは、装置110bが再度初期化されるべきであることを示すことができる。また要求171は、リモートプロセッサ157に情報を送出手、ローカルプロセッサ122Aを指示することができる。例えば、サポートアプリケーション160は、ローカルプロ

セッサ122A及び装置110bの構成に関する付加情報を必要とする場合もある。ローカルプロセッサ122Aは、応答172において要求された情報を送出手。

【0032】応答172は、プロキシ装置145がリモートプロセッサ157からローカルプロセッサ122Aに別の「応答」メッセージをルーティングするのを認可するHTTPヘッダのプロキシ情報を含む。その後、リモートプロセッサ157は、要求173を送出手、その要求を、プロキシ装置145がローカルプロセッサ122Aにルーティングする。要求173は、装置110bに対して実行されるべきコマンドを指示することができ、またローカルプロセッサ122Aを指示して、リモートプロセッサ157にさらに情報を与えることができる。要求173がローカルプロセッサ122が付加情報を送出手する指示を含む場合には、ローカルコンピュータは、応答174においてその付加情報を送出手。

【0033】この要求及び応答のパターンは、図2の内容に則して上で説明したものと同様である。ローカルプロセッサ122Aによって、リモートプロセッサ157に送出手される各メッセージ（要求170及び応答172、174）は、プロキシ装置145がメッセージ（要求171及び173）をリモートプロセッサ157からローカルプロセッサ122Aにルーティングするのを認可するHTTPヘッダのプロキシ情報を含む。それにより装置110bは、リモートプロセッサ157から間接的に制御される。

【0034】図4は、本発明による、全体的に参照番号200によって示される装置管理プロセスの論理ステップを示す。上記のように、装置管理プロセス200は、利用者によって起動される通信開始コマンド130、Eメール通信開始コマンド140或いは装置によって起動される通信開始コマンド113によって開始することができる。それぞれの場合に、装置管理プロセス200は、ステップ210で開始し、ステップ215に進む。

【0035】ステップ215では、ローカルプロセッサがリモートプロセッサにメッセージを送出手、またプロキシ装置がリモートプロセッサからローカルプロセッサにメッセージをルーティングするのを認可する。ローカルプロセッサからのメッセージは、ローカルプロセッサとリモートプロセッサとの間で通信を開始することを意図しており、典型的には、ローカルプロセッサ及び管理されるべき装置に関する構成情報を含む。

【0036】ステップ220では、ローカルプロセッサはリモートプロセッサからメッセージを受信する。リモートプロセッサからのメッセージは、ローカルプロセッサによって実行されるべき1つ或いは複数のコマンドを指示する。

【0037】ステップ225では、ローカルプロセッサは、ステップ220においてリモートプロセッサからのメッセージにおいて指示されたコマンドを実行する。例

えば、そのコマンドは、特定の装置の構成状態を読み出すことを要求したり、或いは装置を再度初期化するように能動的な動作を実行することを要求する場合もある。

【0038】ステップ230では、ローカルプロセッサはさらにリモートプロセッサからのメッセージを評価し、リモートプロセッサに別のメッセージを送出するように、リモートプロセッサがローカルプロセッサに要求しているか否かを判定する。例えば、リモートプロセッサからの以前のメッセージによって、装置の較正が開始されていると、リモートプロセッサは、ここで、較正が成功したか否かを判定するために、あるフィードバック情報を必要とする。

【0039】ステップ230の間に行われる判定によって、リモートプロセッサは、ローカルプロセッサとのメッセージ交換を継続するか否かを制御できるようになる。プロキシ装置は、認可を受けた場合にのみ、メッセージをリモートプロセッサからローカルプロセッサにルーティングし、またその認可はメッセージ毎に必要なことを思い起こされたい。従って、リモートプロセッサからローカルプロセッサに送出される全てのメッセージの前に、ローカルプロセッサからプロキシ装置に対して認可が行われなければならない。リモートプロセッサがローカルプロセッサとの通信の保持を望む場合には、ローカルプロセッサへの各メッセージにおいて、リモートプロセッサは、ローカルプロセッサがリモートプロセッサに対して別のメッセージを送出するように指示しなければならない。

【0040】リモートプロセッサからのメッセージが、ローカルプロセッサが別のメッセージを送出しなければならないことを示す場合には、そのプロセスはステップ235に進み、そうでない場合には、そのプロセスはステップ250に進む。

【0041】ステップ235では、ローカルプロセッサは、次のメッセージをリモートプロセッサに送出し、またプロキシ装置が次のメッセージをリモートプロセッサからローカルプロセッサにルーティングするのを認可する。

【0042】ステップ240では、ローカルプロセッサは、リモートプロセッサから次のメッセージを受信する。このリモートプロセッサからのメッセージは、ローカルプロセッサによって実行すべき1つ或いは複数のコマンドを指示する。

【0043】ステップ245では、ローカルプロセッサは、ステップ240においてリモートプロセッサからのメッセージで指示されたコマンドを実行する。その後そのプロセスは、ステップ230に戻って繰り返される。

【0044】ステップ250において、そのプロセスは終了する。

【0045】上記のように、リバーストンネリングプロトコルは、ウェブブラウザによって、ファイヤウォール

で保護されたウェブサイトを見るための簡単な機構を提供する。それは、ファイヤウォールが通過を許可する形態でウェブトラフィック要求及び応答を送信するシステムを実現するプロトコルである。上述の各実施形態では、ウェブサイト上で動作するアプリケーションは、トンネリングプロトコルを組み込むために変更される必要があった。多数のアプリケーションを変更するのを避けるために、図5は、個別のプロキシ装置を用いてファイヤウォールへのインターフェースを提供する、本発明の実施形態を示す。サーバ、ブラウザ、及び他のウェブサイト上で動作するアプリケーションがそのプロトコルを実施する代わりに、これらのプロキシ装置がリバースHTTP通信プロトコルを実施する。

【0046】以下の記載からわかるように、図5の実施形態によって、ファイヤウォール内のエンティティは、ファイヤウォール外部のエンティティにアクセスを提供できるようになる。さらに、ファイヤウォール内部のエンティティは、リバースhttpプロトコルセッションを何時でも終了し、ファイヤウォールの外部のウェブブラウザが、ファイヤウォール内部の装置にアクセスするのを防ぐことができる。

【0047】コンピュータシステム300は、ファイヤウォール305の内側302とファイヤウォール305の外側304との間に介在するファイヤウォール305を備える。内側302は、ウェブサーバ308Iと、ブラウザ314Iと、アプリケーション316Iとに接続されるプロキシエージェント306を備える。同様に、外側304は、ウェブサーバ308Eと、ブラウザ314Eと、アプリケーション316Eとに接続されるリバースプロキシ312を備える。内側302では、ファイヤウォール305は、プロキシエージェント306に接続され、外側304では、ファイヤウォール305は、インターネットのようなコンピュータネットワーク301を介してリバースプロキシ312に接続される。ファイヤウォール305によって、内側302の装置は、外側304の装置から発信される不要な通信から保護される。

【0048】リバースプロキシエージェント306は、ファイヤウォール305と1つ或いは複数のウェブサーバ308Iとの間のインターフェースを形成する。各ウェブサーバ308Iは、1つ或いは複数のパーソナルコンピュータ(PC)310Iと通信を行う。各PC310Iは、HTTPプロトコルに準拠する通信プログラムを組み込んでいる。プロキシエージェント306は、各ウェブサーバ308Iとファイヤウォール305とのインターフェースを形成する役割を担う。リバースプロキシエージェント306(以下、「エージェント」)は、ウェブサーバ308Iから受信する要求に応じて、ファイヤウォールを介して、ファイヤウォール305の外側304に配置されるリバースプロキシ装置312との接

続を開始する。この接続は、利用者が接続を閉じるまで、開いたままである。

【0049】エージェント306の別の機能は、接続を介して外部装置から受信したブラウザ要求を抽出し、その要求を、適当なウェブサーバ308Iに転送することである。例えば、エージェント306は、ファイヤウォール305の外側304に位置するブラウザ314Eの代わりに、ウェブサーバ308Iへの要求を行う。エージェント306の別の機能は、ブラウザ314Eからの次の応答がファイヤウォール305によって確実に渡されるように、ウェブサーバ308Iから受信した応答を要求として符号化することである。

【0050】リバースプロキシ312はまた、1つ以上のブラウザ314Eから受信した要求を、ファイヤウォール305によって遮断されることになる要求としてではなく応答としてファイヤウォール305によって認識されるコードによって「包む(wrap)」よう機能する。またリバースプロキシ312は、それぞれ接続の状態を保持し、エージェント306のような、どのエージェントが、プロキシとの接続を開始しているかを記憶し、ウェブサーバ308Iのような、どのサーバがアクセス可能であるかを認識する。同様に、リバースプロキシ312は、ブラウザ314Eのような、どのブラウザがプロキシとの接続を開いているかを記憶する。リバースプロキシ312は、エージェント306と同様にして、ブラウザ314Eから受信した要求を応答に変換し、エージェント306が、リバースプロキシ312から受信した応答を、その後、指示されたウェブサーバ308Iにディスパッチされる要求に変換するリバース機能を実行する。リバース方向では、エージェント306は、ウェブサーバ308Iから受信した応答を要求に変換し、その要求をファイヤウォール305を介してリバースプロキシサーバ312にディスパッチする。要求を受信すると、リバースプロキシ312は「包みを解いて」に、応答を適当なブラウザ314Eにディスパッチする。

【0051】このようにして、ファイヤウォール305の保護機能は、エージェント306及びリバースプロキシ312の包み込み動作によってバイパスされる。接続を確立する初期要求を除いて、エージェント306は、内側302から受信した応答を要求のように見せるとともに、ファイヤウォール305から受信した応答を要求に変換する。同様に、リバースプロキシ312は、ファイヤウォール305から受信した要求を、要求を出しているブラウザ314Eにディスパッチするための応答に変換するとともに、ブラウザ314Eから受信した要求を応答のように見せる。

【0052】内側或いは外側のような構成要素の呼び方は、単なる1つの見方にすぎないことに留意されたい。また通信は、ウェブサーバ308Eに接続されるPC310Eとブラウザ314Iとの間にも確立できる。その

ような場合には、PC310E、ウェブサーバ308E及びブラウザ314Iの機能は、それぞれ上記のようなPC310I、ウェブサーバ308I及びブラウザ314Eの機能と同様であり、エージェント306及びリバースプロキシ312の機能的な役割は逆になる。

【0053】リバースプロキシ312及びエージェント306の規定によって、ブラウザ314I、314E及びウェブサーバ308I、308Eは、リバーストンネリング手順を全く知らなくても済むようになる。またその手順は、それぞれエージェント306及びリバースプロキシ312とのインターフェースを直接形成する316I及び316Eのようなアプリケーションに対して透過性がある。従って、本発明は、アプリケーション316I、316Eと、PC310I、310E上で動作するアプリケーションと、ウェブサーバ308I、308Eと、ブラウザ314I、314Eに関して、コードの変更或いは追加の修正を行うことなく、実施される。エージェント306及びリバースプロキシ312は、完全にソフトウェアで実施し、ファイヤウォール305と同様の機器上に常駐させるか、個別の機器に常駐させることもできる。

【0054】上記の説明は、本発明の例にすぎないことを理解されたい。当業者は、本発明から逸脱することなく、種々の変更形態及び変形形態を考案することができるであろう。例えば、管理されている装置は、任意のコンピュータ周辺機器、別のコンピュータ、或いはローカルプロセッサそのものとすることができる。また、ファイヤウォール或いはプロキシ装置を備えないシステムの場合には、プロキシ装置がメッセージをローカルプロセッサにルーティングするのを認可するステップを単に削除するだけで、その手順を適用することができる。さらに、本発明を実行するために必要とされるプロセスは、ローカルコンピュータのメモリに予めロードされているものとして示されるが、後にローカルコンピュータにロードするために、図2のデータメモリ115及び図3のデータメモリ115Aのような記憶媒体上で構成されることもできる。従って、本発明は、添付の請求の範囲の中に入る全ての別形態、変更形態及び変形形態を含むものである。

【0055】以上、本発明の実施例について詳述したが、以下、本発明の各実施態様の例を示す。

【0056】【実施態様1】リモートプロセッサ(314E)が、リバースプロキシ装置(312)と、コンピュータネットワーク(301)と、ファイヤウォール(305)と、プロキシエージェント装置(306)とを介してローカルプロセッサ(308I)に結合される場合に、前記リモートプロセッサ(314E)が前記ローカルプロセッサ(308I)と通信できるようにするトンネリング動作を可能にするための方法であって、ローカル要求メッセージを前記プロキシエージェント装置(3

06) にディスパッチさせて前記リモートプロセッサ (314E) との通信チャネルを確立するよう、前記ローカルプロセッサ (308I) を制御するステップであって、前記プロキシエージェント装置 (306) は前記ファイアウォール (305) と前記ネットワーク (301) とを介して前記ローカル要求メッセージを前記リバースプロキシ装置 (312) にディスパッチし、前記ファイアウォール (305) は前記プロキシエージェント装置 (306) によって前記ローカル要求メッセージに対するリモート応答メッセージを受信することができるようになされる、制御ステップと、前記通信チャネルの確立に基づき、前記リモートプロセッサ (314E) が前記リバースプロキシ装置 (312) にリモート要求メッセージを送出するのを可能にし、次に、前記リバースプロキシ装置 (312) が、前記リモート要求メッセージの中に含んだリモート応答メッセージをディスパッチするのを可能にするステップと、前記ファイアウォール (305) を介して前記プロキシエージェント装置 (306) が前記リモート応答メッセージを受信したときに、前記リモート要求メッセージを抽出して該リモート要求メッセージを前記ローカルプロセッサ (308I) にディスパッチするよう前記プロキシエージェント装置 (306) を制御するステップと、を備えて成り、前記プロキシエージェント装置 (306) 及び前記リバースプロキシ装置 (312) が、前記ローカルプロセッサ (308I) または前記リモートプロセッサ (314E) のいずれかにおける通信アプリケーションを変更することなく、前記トンネリング動作を可能にすることを特徴とする方法。

【0057】[実施態様2]ローカル応答メッセージをローカル要求メッセージに組み込み、前記ローカル要求メッセージを前記ファイアウォール (305) と、前記ネットワーク (310) と、前記リバースプロキシ装置 (312) とを介して前記リモートプロセッサ (314E) にディスパッチすることにより、前記リモート要求メッセージに対する前記ローカルプロセッサ (308I) からの前記ローカル応答メッセージの受信にตอบสนองするよう前記プロキシエージェント装置 (306) を制御するステップであって、前記ファイアウォール (305) は前記ローカル要求メッセージに対するリモート応答メッセージを受信することができるよう前記プロキシエージェント装置 (306) によってなされる、ステップ、をさらに備えて成ることを特徴とする、実施態様1に記載の方法。

【0058】[実施態様3]前記ファイアウォール (305) を介して前記リバースプロキシ装置 (312) が前記ローカル要求メッセージを受信したときに、前記ローカル応答メッセージを抽出して該ローカル応答メッセージを前記リモートプロセッサ (314E) にディスパッチするよう前記リバースプロキシ装置 (312) を制御

するステップ、をさらに備えて成ることを特徴とする、実施態様2に記載の方法。

【0059】[実施態様4]前記コンピュータネットワーク (301) は、インターネットであり、前記プロキシエージェント装置 (306) と前記リバースプロキシ装置 (312) との間でディスパッチされるメッセージは、HTTPフォーマットで構成されることを特徴とする、実施態様1に記載の方法。

【0060】[実施態様5]リモートプロセッサ (314E) が、コンピュータネットワーク (301) と、ファイアウォール (305) とを介して、ローカルプロセッサ (308I) に結合される場合に、前記リモートプロセッサ (314E) が前記ローカルプロセッサ (308I) と通信できるようにするトンネリング動作を可能にするシステムであって、前記ローカルプロセッサ (308I) からのローカル要求にตอบสนองして前記ファイアウォール (305) を介してローカル要求メッセージをディスパッチすることにより、前記リモートプロセッサ (314E) との通信チャネルを確立するプロキシエージェント手段 (306) であって、前記ファイアウォール (305) は前記ローカル要求メッセージに対するリモート応答メッセージを受信することができるよう前記プロキシエージェント手段 (306) によってなされる、プロキシエージェント手段と、前記ローカル要求メッセージの受信と、前記リモートプロセッサ (314E) からのリモート要求メッセージの受信とにตอบสนองして、前記リモート要求メッセージの中に含んだリモート応答メッセージをディスパッチするリバースプロキシ手段 (312) と、を備えて成り、前記ファイアウォール (305) を介して前記プロキシエージェント手段 (306) が前記リモート応答メッセージを受信したときに、前記プロキシエージェント手段 (306) は、前記リモート要求メッセージを抽出して該前記リモート要求メッセージを前記ローカルプロセッサ (308I) にディスパッチし、それにより、前記プロキシエージェント手段 (306) 及び前記リバースプロキシ手段 (312) が、前記ローカルプロセッサ (308I) または前記リモートプロセッサ (314E) のいずれかにおける通信アプリケーションを変更することなく、前記トンネリング動作を可能にすることを特徴とするシステム。

【0061】[実施態様6]前記ローカル応答メッセージをローカル要求メッセージに組み込み、前記ローカル要求メッセージを前記ファイアウォール (305) と、前記ネットワーク (310) とを介して、前記リバースプロキシ手段 (312) にディスパッチすることにより、前記プロキシエージェント手段 (306) は前記リモート要求メッセージに対する前記ローカルプロセッサ (308I) からの前記ローカル応答メッセージの受信にตอบสนองし、前記ファイアウォール (305) は前記ローカル要求メッセージに対するリモート応答メッセージを受信

することができるよう前記プロキシエージェント手段(306)によってなされることを特徴とする、実施態様5に記載のシステム。

【0062】【実施態様7】前記リバースプロキシ手段(312)が、前記ファイアウォール(305)を介して前記ローカル要求メッセージを受信したとき、前記リバースプロキシ手段(312)は、前記ローカル応答メッセージを抽出して該ローカル応答メッセージを前記リモートプロセッサ(314E)にディスパッチすることを特徴とする、実施態様6に記載のシステム。

【0063】【実施態様8】前記コンピュータネットワーク(301)はインターネットであり、前記プロキシエージェント手段(306)と前記リバースプロキシ手段(312)との間でディスパッチされるメッセージは、HTTPフォーマットで構成されることを特徴とする、実施態様5に記載のシステム。

【0064】

【発明の効果】以上説明したように、本発明を用いることにより、インターネットとローカルコンピュータシステムとの間にファイアウォールが介在する通信において、ローカルコンピュータシステム或いはリモートコン

ピュータシステムのいずれかにおいて動作するアプリケーションを変更せずに、リモートコンピュータシステムがインターネットを介してローカルコンピュータシステムにアクセスすることができる。

【図面の簡単な説明】

【図1】従来技術による、プロキシ装置を介してインターネットに接続されるローカルコンピュータを備えるコンピュータシステムのブロック図である。

10 【図2】特に本発明を実行するように構成されたコンピュータシステムのブロック図である。

【図3】本発明を実行するためのコンピュータシステムの別の実施形態のブロック図である。

【図4】本発明の方法を示す流れ図である。

【図5】本発明の別の実施形態のブロック図である。

【符号の説明】

301：コンピュータネットワーク

305：ファイアウォール

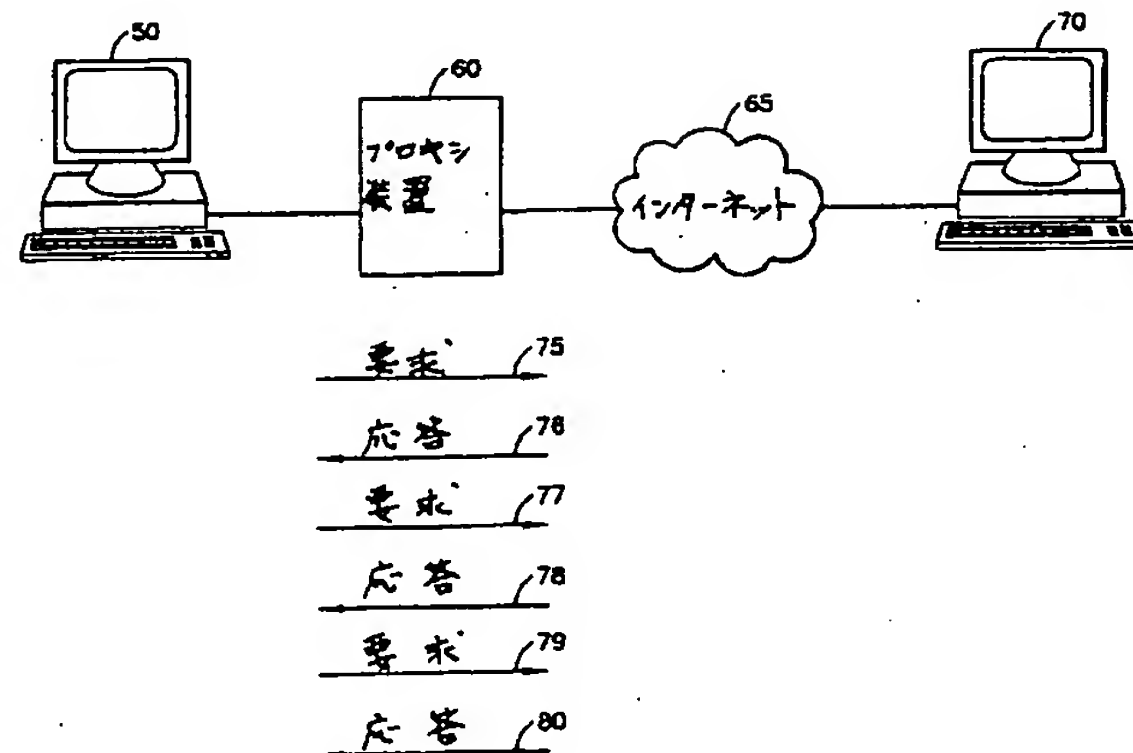
306：プロキシエージェント装置

308I：ローカルプロセッサ

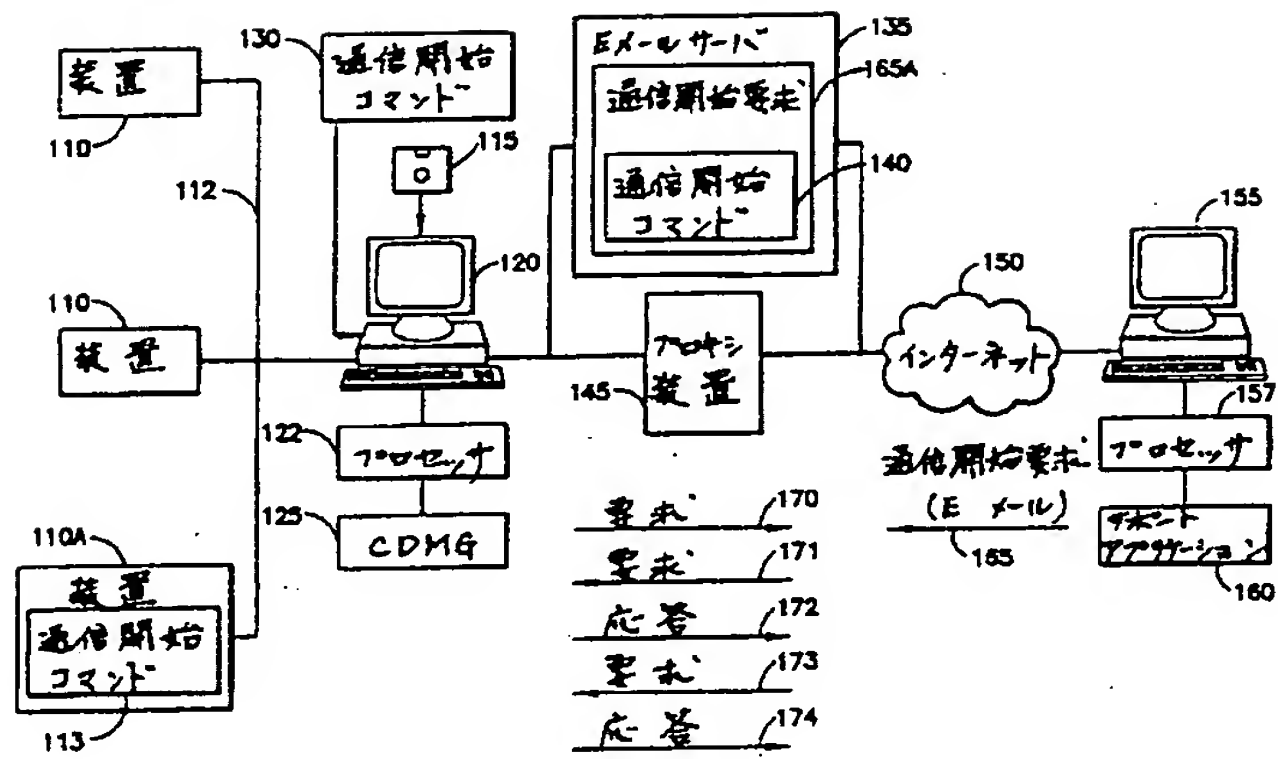
20 312：リバースプロキシ装置

314E：リモートプロセッサ

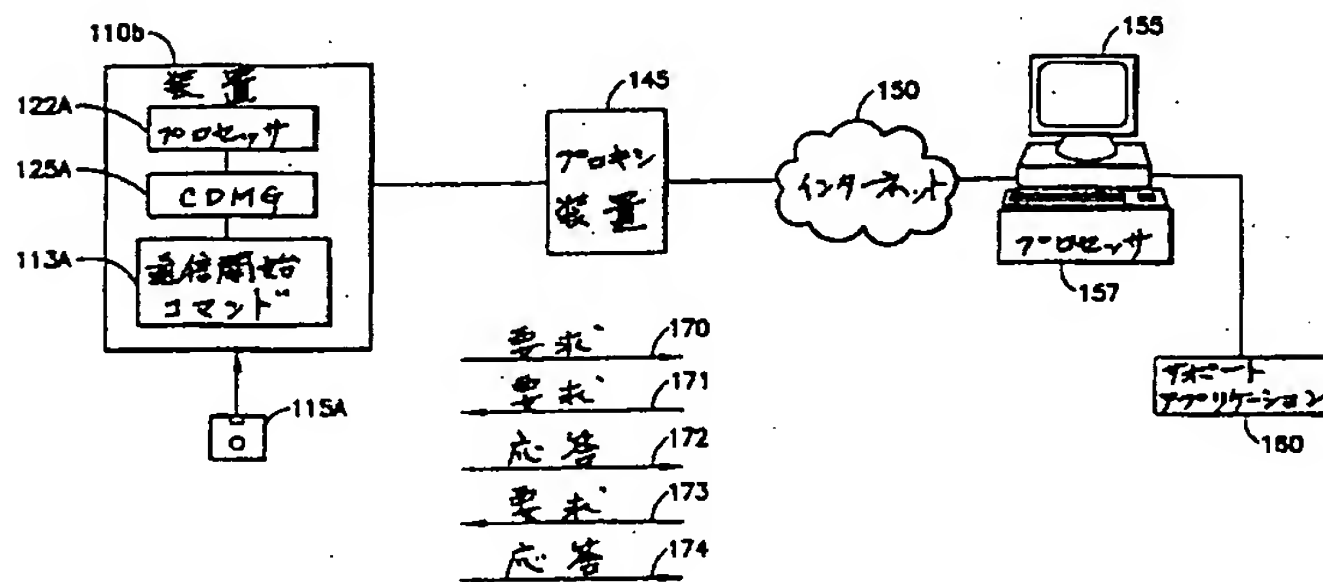
【図1】



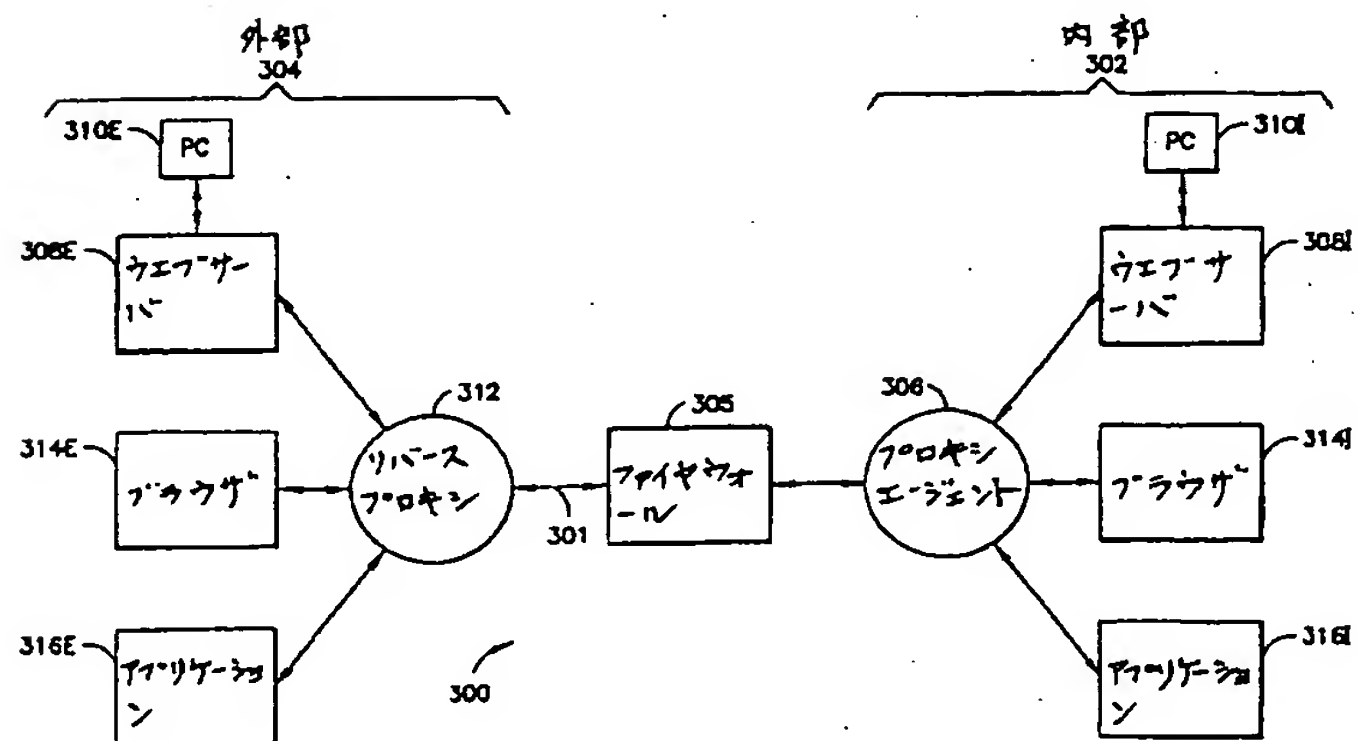
【图2】



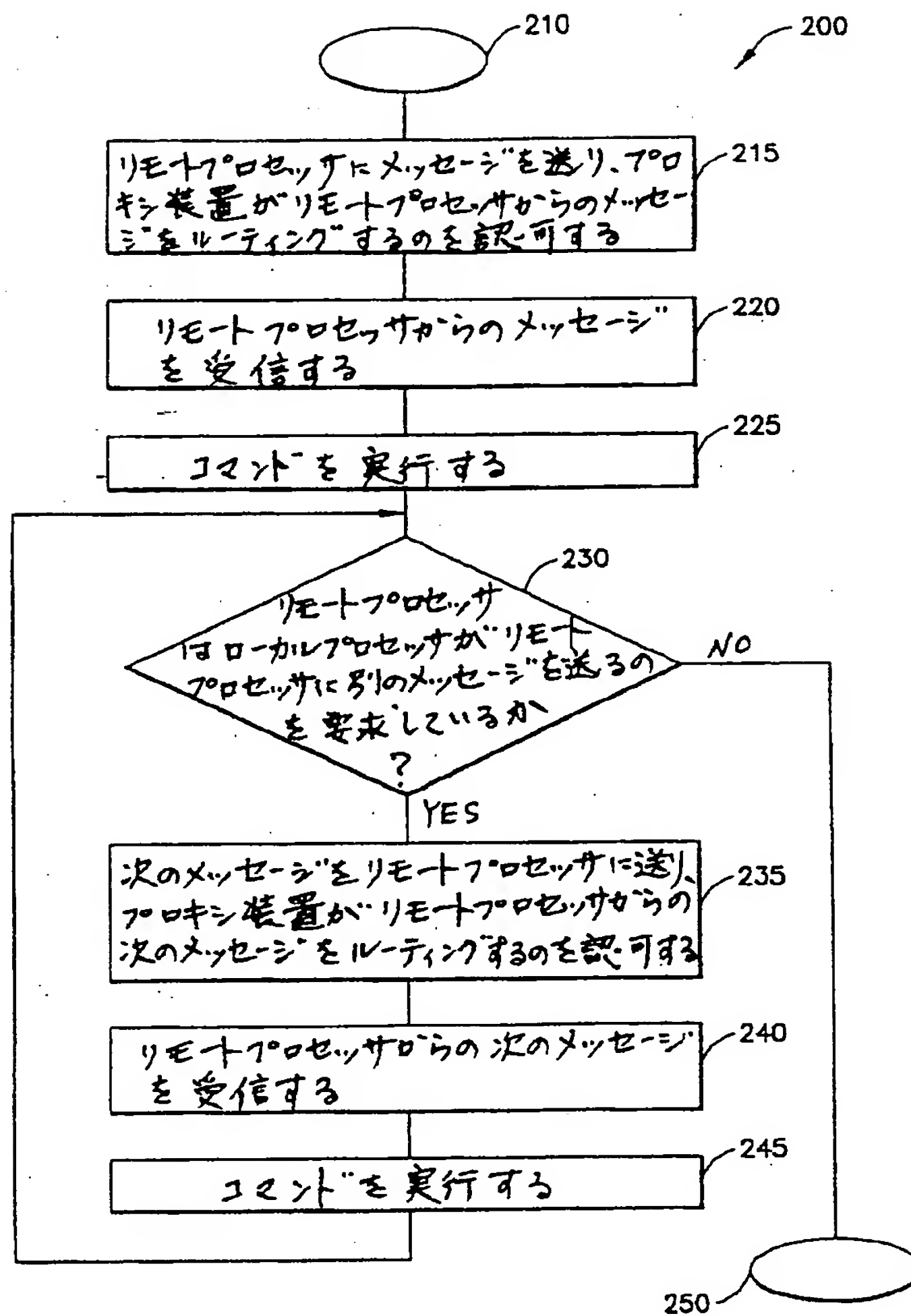
【图3】



【図5】



【図4】



フロントページの続き

(72)発明者 ジェイムス・クラフ
アメリカ合衆国アイダホ州メリディアン
イースト・ウェイクリー・ストリート
465

(72)発明者 ディーン・エス・ネルソン
アメリカ合衆国アイダホ州メリディアン
ウエスト・ブルー・クリーク ドライブ
4049